CLAIMS

What is claimed is:

1. A method of implementing a cellular automata based random number generator (CA-based RNG), comprising:

determining an interconnection topology;

screening a CA-based RNG candidate based on said interconnection topology; and

subjecting said CA-based RNG candidate to a suite of random number tests in response to said CA-based RNG passing said screening step.

2. The method of claim 1, wherein said CA-based RNG candidate is under a periodic boundary condition in at least one dimension.

3. The method of claim 1, wherein said interconnection topology is identical for all cells of said CA-based RNG candidate.

4. The method of claim 1, wherein said determining topology (310) step includes:

exhaustively providing all possible interconnection topologies for a given neighborhood number for cells of said CA-based RNG candidate.

5. The method of claim 4, wherein said determining topology (310) step further includes:

pruning said interconnection topologies to reject interconnection topologies for which no input of a cell of said CA-based RNG candidate is connected to said cell's output.

6. The method of claim 4, wherein said determining topology (310) step further includes:

pruning said interconnection topologies to reject interconnection topologies for which displacement values for all inputs for a cell are evenly divisible by a length of said CA-based RNG for any displacement values whose absolute value is greater than 1.

7. The method of claim 1, wherein said screening (320) step includes:

calculating entropy of said CA-based RNG candidate; and

accepting said CA-based RNG candidate for testing based on one or more predetermined criteria.

8. The method of claim 7, wherein said calculating entropy step includes:

calculating an expected value of a subsequence within a sequence;

initializing said CA-based RNG candidate through a predetermined number of clock cycles and monitoring occurrences of said subsequence; and

determining said entropy based on said expected value and results of monitoring said subsequence occurrences.

9. The method of claim 8, further comprising:

rejecting said CA-based RNG in response said occurrence being greater than a multiple of said expected value.

10. The method of claim 7, wherein said accepting step includes accepting said CA-based RNG candidate for testing in response to said CA-based RNG candidate being in a list of a predetermined number of highest entropy CA-based RNG candidates.

11. The method of claim 10, wherein said accepting step includes accepting said CA-based RNG candidate for testing in response to said entropy of said CA-based RNG candidate being at or above a predetermined threshold entropy.

12. The method of claim 1, wherein said standardized suite of random number tests includes the DIEHARD suite of tests.

13. The method of claim 1, further comprising:

selecting said CA-based RNG candidate in response to said CA-based RNG candidate passing said suite of random number tests without at least one of time spacing and site spacing.

14. A cellular automata based random number generator (CA-based RNG) implementing-module, comprising:

an interconnection-topology-determining-module determining an interconnection topology;

a screening-module screening a CA-based RNG candidate based on said interconnection topology; and

a testing-module subjecting said CA-based RNG candidate through a suite of tests in response to said CA-based RNG passing through said screening-module.

15. The CA-based RNG implementing-module of claim 13, wherein said screening-module comprises:

an entropy-calculating-module calculating entropy of said CA-based RNG candidate; and

a sorting-module accepting or rejecting said CA-based RNG candidate for testing based on a predetermined criteria.

16. The CA-based RNG implementing-module of claim 15, wherein said entropy-calculating-module comprises:

an expected-value-module calculating an expected count value of subsequences within a sequence;

an accumulating-module accumulating actual counts of said subsequences; and

an entropy-determining-module determining said entropy based on an output or outputs of said accumulating-module;

17. The CA-based RNG implementing-module of claim 15, wherein said sorting-module accepts said CA-based RNG candidate for testing in response to said CA-based RNG candidate being in a list of a predetermined number of highest entropy CA-based RNG candidates.

18. The CA-based RNG implementing-module of claim 15, wherein said sorting-module accepts said CA-based RNG candidate for testing in response to said entropy of said CA-based RNG candidate being at or above a predetermined threshold entropy.

19. The CA-based RNG implementing-module of claim 14, wherein said interconnection-topology-determining-module comprises:

a topology-generation-module generating one or more interconnection topologies; and

a topology-pruning-module pruning said interconnections based on one or more predetermined criteria.

20. The CA-based RNG implementing-module of claim 19, wherein said topology-generation-module exhaustively provides all possible interconnection topologies for a given neighborhood number for cells of said CA-based RNG candidate.

21. The CA-based RNG implementing-module of claim 19, topology-pruning-module prunes said interconnection topologies to reject interconnection topologies for which no input of a cell of said CA-based RNG candidate is connected to said cell's output.

22. The CA-based RNG implementing-module of claim 19, topology-pruning-module prunes said interconnection topologies to reject interconnection

topologies for which displacement values for all inputs for a cell are evenly divisible by a length of said CA-based RNG for any displacement values whose absolute value is greater than 1.